MALWARE DISTRIBUTION TRENDS & ASSOCIATED NETWORK TRAFFIC

Brad Duncan
Palo Alto Networks

MALWARE-TRAFFIC-ANALYSIS.NET
Disclaimer

• Timeframe: October & November 2017
• Things can and do quickly change
• Personal bias
Overview

• Types of malware
• Distribution methods
• Network Security Monitoring (NSM) and investigating suspicious activity
• Prevention strategies
Types of malware

• In wide-scale distribution, we most often find:
  • Backdoor Trojans
  • Information stealers
  • Malware downloaders
  • RANSOMWARE
Ransomware is a term for malicious software (malware) that holds your computer or files on your computer for ransom.
Bitcoin rates

1 Bitcoin equals:

- 150,466 Kč
- € 5,869
- $ 6,950
WannaCry
### WannaCry

Filter: `ssl_handshake.type == 1`

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Dst</th>
<th>Port</th>
<th>Info</th>
<th>Server Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-11-10 21:34:31</td>
<td>199.254.238.52</td>
<td>443</td>
<td>Client Hello</td>
<td><a href="http://www.oqllyykb4c2cxt6x.com">www.oqllyykb4c2cxt6x.com</a></td>
</tr>
<tr>
<td>2017-11-10 21:34:31</td>
<td>93.180.156.84</td>
<td>9001</td>
<td>Client Hello</td>
<td><a href="http://www.zsepqqr.com">www.zsepqqr.com</a></td>
</tr>
<tr>
<td>2017-11-10 21:34:37</td>
<td>213.239.217.18</td>
<td>1337</td>
<td>Client Hello</td>
<td><a href="http://www.umpbfly4e.com">www.umpbfly4e.com</a></td>
</tr>
<tr>
<td>2017-11-10 21:34:38</td>
<td>185.96.180.164</td>
<td>443</td>
<td>Client Hello</td>
<td><a href="http://www.gd4dp6r.com">www.gd4dp6r.com</a></td>
</tr>
<tr>
<td>2017-11-10 21:34:39</td>
<td>81.6.36.108</td>
<td>9001</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>199.254.238.52</td>
<td>443</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>93.180.156.84</td>
<td>9001</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>213.239.217.18</td>
<td>1337</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>185.96.180.164</td>
<td>443</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>195.113.199.99</td>
<td>9001</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>81.6.36.108</td>
<td>9001</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Bad Rabbit

http://1dnscontrol.com/flash_install.php
Bad Rabbit

Oops! Your files have been encrypted.

If you see this text, your files are no longer accessible. You might have been looking for a way to recover your files. Don't waste your time. No one will be able to recover them without our decryption service.

We guarantee that you can recover all your files safely. All you need to do is submit the payment and get the decryption password.

Visit our web service at caforsztxqzf2nm.onion

Your personal installation key#1:

2lI6UK78bY69WxwpFBkk9/NxNvki0ZVkJw8XZeyohJjfDPzxPQGB0T/UQw0rr1gMk
r6TeB1pxUWykrAd6dEXx31qquwChxk/sTQIqXi1WXJuomj4iLlvyTqUDhv1Tv1WdGF
a20U8RjQkhZ6qo9ce8dtU/Fh7Ma1NP3RUCvBB+4z3m1FheMYMMvMvTosy8aV5/fdc
0R5YLTixXjLGs4dp+tQ4w9/PvHe4Q6+br02EkZySmMCDxv+BLXuPQl/neVuUWDkL
Ndo1lgb+CHHF5tuk0+jJH3p4UKnyrD058dfiQ1bVZb8J8K010F98Grd0ys1F+F/
GkqwawrIB1TuTj8xEyWhqXHeAtC9967RGA==

If you have already got the password, please enter it below.
Password#1: _
BAD RABBIT

If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you’ll be provided with a bitcoin account to transfer payment. The current price is on the right.

Once we receive your payment you’ll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.

Time left before the price goes up

40:48:22

Price for decryption:

Bitcoin = 0.05

Enter your personal key or your assigned bitcoin address.
Bad Rabbit

- TCP connection attempts via port 80, 139 and 445

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Src</th>
<th>port</th>
<th>Dst</th>
<th>port</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-11-10 22:30</td>
<td>10.11.10.101</td>
<td>49271</td>
<td>10.11.10.1</td>
<td>445</td>
<td>49271-microsoft-ds [SYN]</td>
</tr>
<tr>
<td>2017-11-10 22:30</td>
<td>10.11.10.101</td>
<td>49273</td>
<td>10.11.10.1</td>
<td>445</td>
<td>49273-microsoft-ds [SYN]</td>
</tr>
<tr>
<td>2017-11-10 22:30</td>
<td>10.11.10.101</td>
<td>49274</td>
<td>10.11.10.1</td>
<td>139</td>
<td>49274-netbios-ssn [SYN]</td>
</tr>
<tr>
<td>2017-11-10 22:31</td>
<td>10.11.10.101</td>
<td>49271</td>
<td>10.11.10.1</td>
<td>445</td>
<td>[TCP Retransmission] 492</td>
</tr>
<tr>
<td>2017-11-10 22:31</td>
<td>10.11.10.101</td>
<td>49273</td>
<td>10.11.10.1</td>
<td>445</td>
<td>[TCP Retransmission] 492</td>
</tr>
<tr>
<td>2017-11-10 22:31</td>
<td>10.11.10.101</td>
<td>49274</td>
<td>10.11.10.1</td>
<td>139</td>
<td>[TCP Retransmission] 492</td>
</tr>
<tr>
<td>2017-11-10 22:31</td>
<td>10.11.10.101</td>
<td>49271</td>
<td>10.11.10.1</td>
<td>445</td>
<td>[TCP Retransmission] 492</td>
</tr>
<tr>
<td>2017-11-10 22:31</td>
<td>10.11.10.101</td>
<td>49273</td>
<td>10.11.10.1</td>
<td>445</td>
<td>[TCP Retransmission] 492</td>
</tr>
<tr>
<td>2017-11-10 22:31</td>
<td>10.11.10.101</td>
<td>49274</td>
<td>10.11.10.1</td>
<td>139</td>
<td>[TCP Retransmission] 492</td>
</tr>
<tr>
<td>2017-11-10 22:31</td>
<td>10.11.10.101</td>
<td>49292</td>
<td>10.11.10.1</td>
<td>80</td>
<td>49292-http [SYN] Seq=0 W</td>
</tr>
</tbody>
</table>
Locky

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_%28cryptosystem%29
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:

https://www.torproject.org/download/download-easy.html

If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser:
01234567-89AB-CDEF-46E27B75-DF2A16E14A48.asasìn
復号ソフトウェアをご紹介します。- Locky Decryptor™-
はお客様の暗号化されたファイルの復号と管理を行う特別なソフトウェアです。
Locky

Send 0.2 BTC

localbitcoins.com

cex.io

Buy Bitcoins with VISA/MASTERCARD or wire transfer.

The best for Europe.

comjar.com
anxpro.com
bittylicious.com

Send 0.2 BTC to Bitcoin address:
Up next…

• Types of malware
• Distribution methods
• Network Security Monitoring (NSM) and investigating suspicious activity
• Prevention strategies
How is malware spread?

- Email (targeted phishing or malicious spam)
- The web (pop-up browser windows or exploit kits during normal web browsing)
- Social media like Skype or Saleschat
- Attackers breach networks and drop malware
Distribution through Email

Email is the most common method criminals use to send malware.
Distribution through Email

These emails contain:

- Archives with malware executables
- Microsoft Office documents
- Archives with other types of files
- Links to malware
Subject: Your Office 365 Business billing statement marktwain.com is available.

From: "Microsoft Online Team" <microsoft@micro-online.com>

Date: Tue, 14 Nov 2017 19:38 UTC

Distribution through Email

http://lunawomen.com?5o8v43kjIsU8Xt=roger.clemens@marktwain.com
Distribution through Email

statement_655904.doc (221 KB)

from lunawomen.com?
Distribution through Email

Security Warning: Macros have been disabled. Options...
<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Dst</th>
<th>port</th>
<th>Host</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-11-14 20:39</td>
<td>35.198.85.207</td>
<td>80</td>
<td>lunawomen.com</td>
<td>GET /?5o8v43kJIsU8Xt=<a href="mailto:lana.merilee@yahoo.com">lana.merilee@yahoo.com</a></td>
</tr>
<tr>
<td>2017-11-14 20:39</td>
<td>23.23.170.235</td>
<td>80</td>
<td>api.ipify.org</td>
<td>GET / HTTP/1.1</td>
</tr>
<tr>
<td>2017-11-14 20:39</td>
<td>185.187.90.38</td>
<td>80</td>
<td>hegheconekin.com</td>
<td>POST /ls5/forum.php HTTP/1.1 (application/x</td>
</tr>
<tr>
<td>2017-11-14 20:39</td>
<td>77.48.73.29</td>
<td>80</td>
<td>ragnes.cz</td>
<td>GET /1 HTTP/1.1</td>
</tr>
<tr>
<td>2017-11-14 20:39</td>
<td>185.187.90.38</td>
<td>80</td>
<td>hegheconekin.com</td>
<td>POST /mlu/forum.php HTTP/1.0</td>
</tr>
<tr>
<td>2017-11-14 20:39</td>
<td>77.48.73.29</td>
<td>80</td>
<td>ragnes.cz</td>
<td>GET /2 HTTP/1.1</td>
</tr>
<tr>
<td>2017-11-14 20:40</td>
<td>77.48.73.29</td>
<td>80</td>
<td>ragnes.cz</td>
<td>GET /3 HTTP/1.1</td>
</tr>
<tr>
<td>2017-11-14 20:40</td>
<td>185.187.90.38</td>
<td>80</td>
<td>hegheconekin.com</td>
<td>POST /d2/about.php HTTP/1.0</td>
</tr>
<tr>
<td>2017-11-14 20:42</td>
<td>185.187.90.38</td>
<td>80</td>
<td>hegheconekin.com</td>
<td>POST /ls5/forum.php HTTP/1.1 (application/x</td>
</tr>
<tr>
<td>2017-11-14 20:42</td>
<td>185.174.173.6</td>
<td>443</td>
<td>rowrororofrat.com</td>
<td>Client Hello</td>
</tr>
<tr>
<td>2017-11-14 20:42</td>
<td>185.174.173.6</td>
<td>443</td>
<td>rowrororofrat.com</td>
<td>Client Hello</td>
</tr>
<tr>
<td>2017-11-14 20:42</td>
<td>185.174.173.6</td>
<td>443</td>
<td>rowrororofrat.com</td>
<td>Client Hello</td>
</tr>
<tr>
<td>2017-11-14 20:44</td>
<td>185.187.90.38</td>
<td>80</td>
<td>hegheconekin.com</td>
<td>POST /ls5/forum.php HTTP/1.1 (application/x</td>
</tr>
<tr>
<td>2017-11-14 20:46</td>
<td>185.187.90.38</td>
<td>80</td>
<td>hegheconekin.com</td>
<td>POST /ls5/forum.php HTTP/1.1 (application/x</td>
</tr>
<tr>
<td>2017-11-14 20:47</td>
<td>185.174.173.6</td>
<td>443</td>
<td>rowrororofrat.com</td>
<td>Client Hello</td>
</tr>
<tr>
<td>2017-11-14 20:47</td>
<td>185.174.173.6</td>
<td>443</td>
<td>rowrororofrat.com</td>
<td>Client Hello</td>
</tr>
<tr>
<td>2017-11-14 20:47</td>
<td>185.174.173.6</td>
<td>443</td>
<td>rowrororofrat.com</td>
<td>Client Hello</td>
</tr>
<tr>
<td>2017-11-14 20:47</td>
<td>185.174.173.6</td>
<td>443</td>
<td>rowrororofrat.com</td>
<td>Client Hello</td>
</tr>
<tr>
<td>2017-11-14 20:48</td>
<td>185.187.90.38</td>
<td>80</td>
<td>hegheconekin.com</td>
<td>POST /ls5/forum.php HTTP/1.1 (application/x</td>
</tr>
</tbody>
</table>
Distribution through Email

Subject: Invoice UY6026905
From: NoReplyMailbox@objets-d-evasion.com
Date: Tue, 14 Nov 2017 01:35 UTC

Please find Invoice UY6026905 attached.

InvoiceUY6026905.doc
Distribution through Email
Distribution through Email

C:Users[username]\AppData\Local\Temp
Distribution through Email

C:\Users\[username]\AppData\Local\Temp

kb.schuttesystems.net/FGdhbr5?, "sport-market.ru/FGdhbr5?, "kipshagen-ol.de/FGdhbr5?
<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Dst</th>
<th>port</th>
<th>Host</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-11-14 12:51</td>
<td>194.151.161.144</td>
<td>80</td>
<td>kb.schuttesystems.net</td>
<td>GET /FGdhbr5?</td>
</tr>
<tr>
<td>2017-11-14 12:51</td>
<td>64.182.208.182</td>
<td>80</td>
<td>icanhazip.com</td>
<td>GET / HTTP/1.1</td>
</tr>
<tr>
<td>2017-11-14 12:59</td>
<td>187.188.162.150</td>
<td>449</td>
<td></td>
<td>Client Hello</td>
</tr>
<tr>
<td>2017-11-14 13:03</td>
<td>194.87.103.71</td>
<td>449</td>
<td></td>
<td>Client Hello</td>
</tr>
<tr>
<td>2017-11-14 13:03</td>
<td>187.188.162.150</td>
<td>449</td>
<td></td>
<td>Client Hello</td>
</tr>
<tr>
<td>2017-11-14 13:08</td>
<td>194.87.103.71</td>
<td>449</td>
<td></td>
<td>Client Hello</td>
</tr>
<tr>
<td>2017-11-14 13:08</td>
<td>187.188.162.150</td>
<td>449</td>
<td></td>
<td>Client Hello</td>
</tr>
<tr>
<td>2017-11-14 13:08</td>
<td>91.211.247.47</td>
<td>443</td>
<td></td>
<td>Client Hello</td>
</tr>
<tr>
<td>2017-11-14 13:12</td>
<td>95.213.236.131</td>
<td>447</td>
<td></td>
<td>Client Hello</td>
</tr>
<tr>
<td>2017-11-14 13:12</td>
<td>35.176.85.39</td>
<td>80</td>
<td>gilgroup.com</td>
<td>GET /toler.png</td>
</tr>
<tr>
<td>2017-11-14 13:12</td>
<td>91.211.247.47</td>
<td>443</td>
<td></td>
<td>Client Hello</td>
</tr>
</tbody>
</table>
Distribution through Email
Many different types of files are used by criminals to install malware.

Malicious spam with links to malware is harder for security systems to catch.

Some types of malware have defense mechanisms and will act differently if analyzed.
Distribution through Social Media
Distribution through Social Media

好好数字! 好好学习! | 7:30 PM


Today
Distribution through Social Media

Opening IMG040510402016-JPG.scr

You have chosen to open:

**IMG040510402016-JPG.scr**

which is: scr File

from: http://davenportelectric.com

Would you like to save this file?

[Save File] [Cancel]
Distribution through Social Media
Distribution through Social Media
Distribution through the Web
Distribution through the Web

- Unexpected web pages or pop-up windows
- Exploit kits
Distribution through the Web

Adobe Flash Player Update

"Adobe Flash Player" is out of date!

The version of "Adobe Flash Player" on your system does not include the latest security updates and has been blocked. To continue using "Adobe Flash Player", download an updated version (Recommended)

Do you want to run or save adobe_flash_setup.exe (1.21 MB) from downloadfarmlaboratory.com?

This type of file could harm your computer.
Distribution through the Web

The "Mercury Text" font was not found.

The web page you are trying to load is displayed incorrectly, as it uses the "Mercury Text" font. To fix the error and display the next, you have to update the "Mozilla Font Pack".

Manufacturer: Mozilla Corporation.
Current version: Mozilla Font Pack 53.0.2785.89
Latest version: Mozilla Font Pack 57.2.5284.21

Update
Distribution through the Web

The "Mercury Text" font was not found.

The web page you are trying to load is displayed incorrectly, as it uses the "Mercury Text" font. To fix the error and display the next, you have to update the "Chrome Font Pack".

Manufacturer: Google Inc. All Rights Reserved.
Current version: Chrome Font Pack 54.0.2785.89
Latest version: Chrome Font Pack 56.0.2924.87

Update
Distribution through the Web

criminal's malware

behind the scenes

user's computer
Exploit kits are web servers that use exploits to take advantage of vulnerabilities in browser-based applications to infect a Windows computer without the user's knowledge.
Exploit Kits

- Flash player
- Web browser
- Silverlight
- Java, PDF
Normal website → GATE → Malicious AD → Exploit kit server

Exploit Kits
Exploit Kits

Filter: http.request

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Dst</th>
<th>port</th>
<th>Host</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-11-13 02:06</td>
<td>194.58.40.193</td>
<td>80</td>
<td>194.58.40.193</td>
<td>GET /test22.php HTTP/1.1</td>
</tr>
<tr>
<td>2017-11-13 02:06</td>
<td>188.225.84.162</td>
<td>80</td>
<td>188.225.84.162</td>
<td>GET /?Njc5MDQx&amp;bUSAJNpCBE</td>
</tr>
<tr>
<td>2017-11-13 02:06</td>
<td>188.225.84.162</td>
<td>80</td>
<td>188.225.84.162</td>
<td>GET /?NTQ2NTkw&amp;BeQIoyXajre</td>
</tr>
<tr>
<td>2017-11-13 02:06</td>
<td>194.58.40.193</td>
<td>80</td>
<td>194.58.40.193</td>
<td>GET /favicon.ico HTTP/1.1</td>
</tr>
<tr>
<td>2017-11-13 02:06</td>
<td>188.225.84.162</td>
<td>80</td>
<td>188.225.84.162</td>
<td>GET /?NTE2NTY0&amp;nbzaccQbG9</td>
</tr>
<tr>
<td>2017-11-13 02:06</td>
<td>37.48.125.120</td>
<td>80</td>
<td>37.48.125.120</td>
<td>GET /tutu.exe HTTP/1.1</td>
</tr>
</tbody>
</table>
## Exploit Kits

### RealTime Events

<table>
<thead>
<tr>
<th>Dst IP</th>
<th>DPort</th>
<th>Event Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>188.225.84.162</td>
<td>80</td>
<td>ET CURRENT_EVENTS RIG EK URI Struct Jun 13 2017</td>
</tr>
<tr>
<td>87.106.190.153</td>
<td>443</td>
<td>ET TROJAN Win32/Ramnit Checkin</td>
</tr>
<tr>
<td>173.194.55.139</td>
<td>80</td>
<td>ET POLICY exe download via HTTP - Informational</td>
</tr>
<tr>
<td>37.48.125.120</td>
<td>80</td>
<td>ET POLICY Internet Explorer 6 in use - Significant Security</td>
</tr>
<tr>
<td>37.48.125.120</td>
<td>80</td>
<td>ET INFO Executable Download from dotted-quad Host</td>
</tr>
</tbody>
</table>

### Escalated Events

- GET `/?Njc5MDQx&bUSAJNpCBE` from 188.225.84.162
- GET `/?NTQ2NTkw&BeQIoyXajrp` from 188.225.84.162
- GET `/?NTE2NTY0&nbzaccQbG9` from 188.225.84.162
- GET `/tutu.exe` from 37.48.125.120
Up next...

• Types of malware
• Distribution methods
• **Network Security Monitoring (NSM)** and investigating suspicious activity
• Prevention strategies
Monitoring and Investigations
Monitoring and Investigations

- 162.254.150.34 port 80
- 185.202.103.26 port 5000

Event Message

ET POLICY PE EXE or DLL Windows file download
ET SHELLCODE Possible TCP x86 JMP to CALL Shellcode...
ET POLICY Cryptocurrency Miner Checkin
## Monitoring and Investigations

Filter: `http.request or tcp.port eq 5000`

<table>
<thead>
<tr>
<th>Dst</th>
<th>port</th>
<th>Host</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>162.254.150.34</td>
<td>80</td>
<td>bmooc.net</td>
<td>GET /wp-content/service/cat.php?m=f</td>
</tr>
<tr>
<td>162.254.150.34</td>
<td>80</td>
<td>bmooc.net</td>
<td>GET /wp-content/service/cat.php?m=j</td>
</tr>
<tr>
<td>162.254.150.34</td>
<td>80</td>
<td>bmooc.net</td>
<td>GET /wp-content/service/cat.php?m=e</td>
</tr>
<tr>
<td>185.202.103.26</td>
<td>5000</td>
<td></td>
<td>51069→commplex-main [SYN] Seq=0 Win:</td>
</tr>
<tr>
<td>10.11.12.101</td>
<td>51069</td>
<td></td>
<td>commplex-main→51069 [SYN, ACK] Seq=0</td>
</tr>
<tr>
<td>185.202.103.26</td>
<td>5000</td>
<td></td>
<td>51069→commplex-main [ACK] Seq=1 Ack:</td>
</tr>
<tr>
<td>185.202.103.26</td>
<td>5000</td>
<td></td>
<td>unknown 0x69 [Malformed Packet]</td>
</tr>
<tr>
<td>10.11.12.101</td>
<td>51069</td>
<td></td>
<td>commplex-main→51069 [ACK] Seq=1 Ack:</td>
</tr>
<tr>
<td>10.11.12.101</td>
<td>51069</td>
<td></td>
<td>unknown 0x69 [Malformed Packet]</td>
</tr>
<tr>
<td>185.202.103.26</td>
<td>5000</td>
<td></td>
<td>51069→commplex-main [ACK] Seq=173 Ack:</td>
</tr>
<tr>
<td>185.202.103.26</td>
<td>5000</td>
<td></td>
<td>unknown 0x69 [Malformed Packet]</td>
</tr>
<tr>
<td>10.11.12.101</td>
<td>51069</td>
<td></td>
<td>commplex-main→51069 [ACK] Seq=315 Ack:</td>
</tr>
</tbody>
</table>
GET /wp-content/service/cat.php?m=f HTTP/1.1
Host: bmooc.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0)
Gecko/20100101 Firefox/56.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive

Monitoring and Investigations

Date/Time | Dst | port | Info
--- | --- | --- | ---
2017-11-12 21:59 | 185.202.103.26 | 5000 | unknown 0x69 [Malformed Packet]

Follow TCP Stream (tcp.stream eq 9)

Stream Content

```json
{"id":1,"jsonrpc":"2.0","method":"login","params":
{"login":"serezhenka_kozlov_1963@mail.ru","pass":"x","agent":"XMRig/2.3.1 (Windows NT 10.0) libuv/1.13.2-dev msvc/2015"}
{"id":1,"jsonrpc":"2.0","result":
{"id":"6a32d621-600e-419b-8f17-8586d93c9e8e","job":
{"blob":"0606ebfba2d0053d2334f55bb83c1799965a95c86079593b65efcb5e2e912559e661bee800d07000000815f765acc37feddee14b557e016ceab795a002b8bd539283c75257020bb5c8cfd05","job_id":"531685671584386810","target":"7b5e0400"},"status":"OK"}
{"id":2,"jsonrpc":"2.0","method":"keepalive","params":
{"id":"6a32d621-600e-419b-8f17-8586d93c9e8e"}}
{"id":2,"jsonrpc":"2.0","error":null,"result":{"status":"KEEPALIVED"}}
{"id":3,"jsonrpc":2.0,"method":"submit","params":
{"id":"6a32d621-600e-419b-8f17-8586d93c9e8e","job_id":"531685671584386810","nonce":"e80b0081","result":"5740ee2856cd78a3715989e988d9424d8b520446ff7237936ca22a7a01330200"}}
```
Up next…

- Types of malware
- Distribution methods
- Network Security Monitoring (NSM) and investigating suspicious activity
- Prevention strategies
Prevention Strategies

- Regular backups of important data.
- Keep systems up-to-date and fully patched.
- Training and awareness.
- Browsing restrictions.
- Security solutions.
MALWARE DISTRIBUTION TRENDS & ASSOCIATED NETWORK TRAFFIC

Thank you!

Brad Duncan
Threat Intelligence Analyst

unit42